REMARKS

The Examiner has rejected Claims 1-21 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner asserts that applicant's claimed "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar" has not been described in the specification. Applicant respectfully disagrees with such an assertion.

Applicant respectfully points out that in paragraph [0006], it is at least suggested that the problems of paragraph [0005] are overcome by the present invention, thus providing the claimed advantage at issue. Furthermore, such claimed advantage is inherent and therefore should not be considered new matter. See below:

> MPEP 2163.07(a) Inherent Function, Theory, or Advantage
>
> By disclosing in a patent application a device that inherently performs a function or has a property, operates according to a theory or has an advantage, a patent application necessarily discloses that function, theory or advantage, even though it says nothing explicit concerning it. The application may later be amended to recite the function, theory or advantage without introducing prohibited new matter. In re Reynolds, 443 F.2d 384, 170 USPQ 94 (CCPA 1971); In re Smythe, 480 F. 2d 1376, 178 USPQ 279 (CCPA 1973). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted).

The Examiner has also rejected Claims 2, 11, 19, and 21 under 35 U.S.C. 112, second paragraph, for being indefinite. Specifically, the Examiner has stated that it is not clear whether the verifications in applicant's claimed "verifying the hash value" take place at the first node, the second node, or the key distribution center. Applicant respectfully asserts that it is purposefully not claimed at which node the operation takes place in order to provide claim breadth.

The Examiner has rejected Claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Menezes et al., *Handbook of Applied Cryptography*. Applicant respectfully disagrees with such rejection.

The Examiner has persisted with the current rejection. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of dependent Claim 2 et al. into each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on page 503, protocol 12.26, message 1 of Menezes to make a prior art showing of applicant's claimed "sending a first message from the first node to the second node, wherein the first message requests establishing the cryptographic key." Applicant respectfully asserts that Menezes teaches that "A interacts with trusted server T and party B" and that the result is entity authentication between A and B (see page 503, 12.26). There is simply no disclosure of a "first message [that] requests establishing the cryptographic key," as claimed by applicant. Instead, Menezes simply generally teaches that entity authentication is established from A's interaction with T and B.

The Examiner has also relied on page 503, protocol 12.26, message 1 of Menezes to meet applicant's claimed "sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, [and] a second identifier for the second node...". Applicant respectfully asserts that Menezes generally teaches entity authentication between A and B as a result

of A interacting with T and B. Such teaching does not meet applicant's specific claim language since there is no mention of any sort of second message from the second node to a key distribution center. In fact, Menezes discloses that T chooses the session key such that there would be no need for a second message in the manner claimed by applicant and in addition there is clearly not even a suggestion of any sort of "key distribution center," as claimed by applicant.

Further, the Examiner has admitted that Menezes does not explicitly disclose applicant's claimed "message authentication code created using a second node key belonging to the second node" and "recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center."

To meet such language, the Examiner has responded to applicant's arguments by stating that Menezes discloses MAC's (page 361, below definition 9.77) and identity-based keying (page 561, section 13.4.3), and that it would have been obvious to modify the key distribution protocol by including the use of a MAC in order to provide data origin authentication and data integrity, and by including identity based keying in order to prevent forgery and impersonation.

Applicant respectfully disagrees with the Examiner's assertion. Specifically, Menezes simply teaches that one way, out of three possible ways, for providing data origin authentication is carried out by way of MAC's. Such a general disclosure of why MAC's are used simply does not meet applicant's specific claim language. Particularly, there is simply no suggestion in Menezes of any sort of second message that is sent from a second node to a key distribution center, where the second message includes a MAC. Menezes teaches utilizing MAC's between parties sharing a key, and not between a second node and a key distribution center.

In addition, Menezes does not disclose that the MAC is "created using a second node key belonging to the second node," as claimed by applicant. Menezes simply

teaches that the MAC is the shared key, but not that it is created by a key belonging to one of the parties.

Still yet, Menezes identity-based keying (page 561, section 13.4.3) simply does not rise to the level of specificity of applicant's claim language. Identity-based keying does not meet any sort of recreating of a second node key at a key distribution center, in the manner claimed by applicant. Also, general identity-based keying does not even suggest any sort of second node key that was previously created using the second node identifier and a secret key known only to the key distribution center. Thus, clearly applicant's claim language has not been met.

The Examiner has further responded to applicant's arguments by stating that "the fact that applicant has recognized other advantages which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious." Applicant respectfully asserts that the claimed advantages would not flow naturally and also that the difference would not be obvious.

Specifically, applicant previously noted in paragraph [0005] of the originally filed specification that applicant's claimed invention provides a particular advantage over key distribution schemes such Kerberos in that database updates are not required for unfamiliar participants. Since the technique relied upon by Menezes is analogous to Kerberos, it explicitly lacks, and even *teaches away* from, any sort of similar advantage and thus could not flow naturally from the prior art. For these reasons, applicant contends that it would simply not be obvious to modify Menezes to meet applicant's claim limitations noted above.

The Examiner has also responded to applicant's arguments by stating that the amendment made previously with respect to each of the independent claims fails to comply with 37 CFR 1.111(b) since it amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant respectfully points out that again, with applicant's claimed invention, database updates are at least partially not required for unfamiliar participants. Since the technique relied upon by Menezes is analogous to Kerberos, it explicitly lacks, and even *teaches away* from, not requiring database updates for unfamiliar participants.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as suggested by the Examiner. A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

Despite the foregoing stark differences and in the spirit of expediting the prosecution of the present application, applicant now substantially claims the following in each of the independent claims:

"wherein communicating the cryptographic key to the second node and the first node includes:

encrypting a hash value and the cryptographic key using the second node key to create a first encrypted key;

recreating a first node key belonging to the first node, wherein the first node key was previously created using the secret key and the first node identifier;

encrypting the hash value and the cryptographic key using the first node key to create a second encrypted key;

sending a third message from the key distribution center to the second node, wherein the third message includes the first encrypted key and the second encrypted key;

decrypting at the second node the first encrypted key from the third message to recover the hash value and the cryptographic key;

verifying the hash value; and

if the hash value is verified,

sending a fourth message to the first node from the second node, wherein the fourth message includes the second encrypted key and a key confirmation value so that the first node can confirm that the cryptographic key has been established,

decrypting at the first node the second encrypted key from the fourth message to recover the hash value and the cryptographic key,

verifying the hash value,

establishing at the first node that the second node has the cryptographic key, and

if the hash value is verified and it is established at the first node that the second node has the cryptographic key,

sending a fifth message to the second node from the first node so that the second node can confirm that the cryptographic key has been established." (see the same or similar, but not identical language in dependent Claim 2 et al.)

Applicant respectfully emphasizes that the Examiner admits that the protocol in Menezes "does not explicitly disclose recreating a first node key previously created using the first node identifier and the secret key." The Examiner goes on to argue that "Menezes discloses identity-based keying" and further "although the protocol does not explicitly disclose the use of a hash value in the messages for verification, Menezes discloses that hash values can be used for verification of data." The Examiner then

concludes that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the key distribution protocol by including the use of a hash, in order to provide data integrity."

Again, for the reasons set forth hereinabove, not only are applicant's claims not met, but it would be *unobvious* to modify Menezes to meet applicant's claims. Only applicant teaches such specific flow for the purpose of providing a technique wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar.

Again, a notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims dependent therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P254).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100